Clase 5 — 27.11.25

#ciscopackettracer #network

👨‍🏫 **Profesor:** Carlos Quintana
📘 **Unidad:** Ciberseguridad
🗓️ **Fecha:** 27/11/2025
🎯 **Tema:** Firewall físico Cisco ASA, niveles de seguridad, VLAN INSIDE/OUTSIDE y acceso controlado a servidores mediante WebVPN (AAA)

1️⃣ Contexto de la clase

El profesor parte del ejercicio anterior:

- Unión de **dos redes independientes** usando **AAA + IoT + enrutamiento**
- Simulación de **dos viviendas o sedes**
- El ejercicio queda **en pausa** para centrarse en **firewalls**

2️⃣ Antivirus vs Firewall

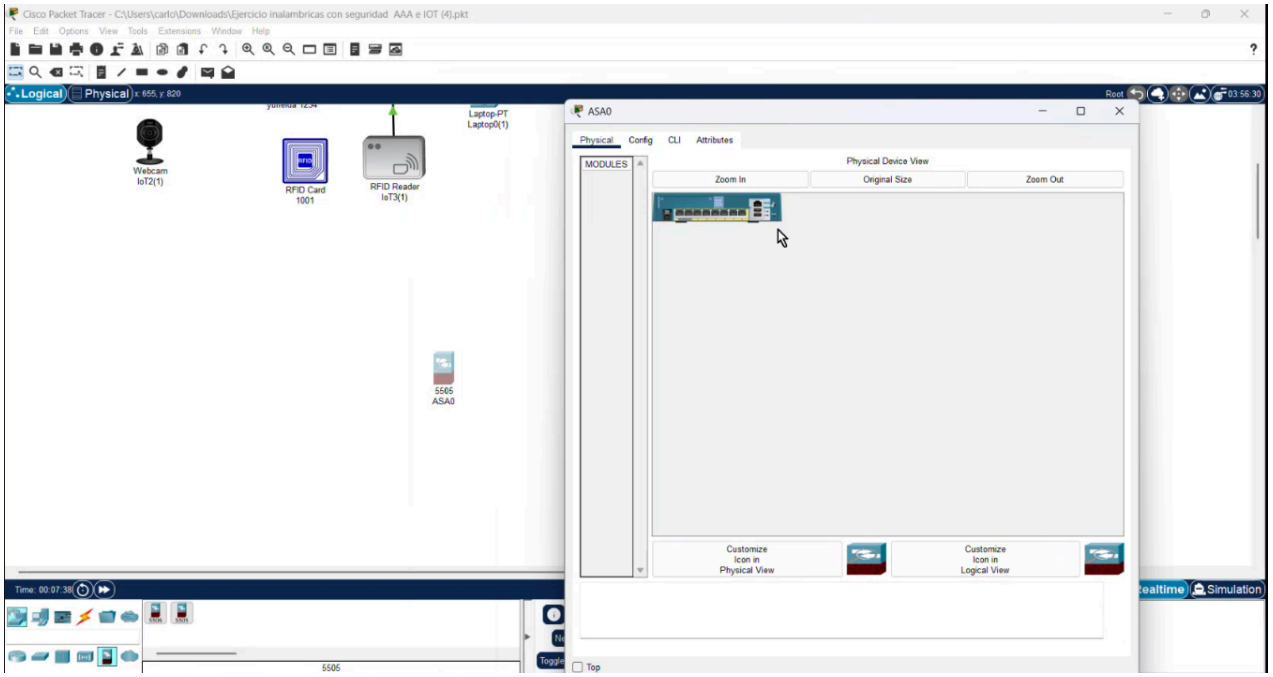
En ciberseguridad es fundamental entender **en qué punto actúa cada mecanismo de defensa**, ya que firewall y antivirus **no compiten**, sino que **se complementan**.

🔹 Firewall

El **firewall** es el **primer filtro de seguridad** de una red o sistema. Su función principal es **controlar el tráfico** que entra y sale, basándose en reglas previamente definidas.

- **Primera línea de defensa**
  El firewall se sitúa *antes* de que el tráfico alcance los sistemas internos. Actúa en el perímetro de la red, evitando que amenazas evidentes lleguen siquiera al sistema operativo o a las aplicaciones.
- Filtra tráfico **antes de entrar al sistema**
  Analiza paquetes según criterios como:
  - IP de origen y destino
  - Puertos
  - Protocolos (TCP, UDP, ICMP…)
  - Interfaces y zonas de seguridad
- Decide **qué entra y qué no**
  No “limpia” virus. Simplemente **permite o bloquea** tráfico.
  Si algo no está permitido explícitamente, **no pasa**.
- Puede ser:
  - 🧠 **Lógico (software)**
    Integrado en el sistema operativo (por ejemplo, el Firewall de Windows). Protege un equipo concreto.
  - 🧱 **Físico (hardware dedicado)**
    Dispositivo independiente (como Cisco ASA). Protege **toda una red**, es más robusto y

escalable.



👉 Por este motivo **las empresas cotizan y utilizan firewalls físicos**.

📌 Idea clave:

> El firewall **no elimina virus**, simplemente intenta que **no entren**.

🔹 Antivirus

El **antivirus** entra en juego **cuando el ataque ya ha superado la barrera perimetral**.

- Actúa **cuando el malware ya ha entrado**
  Analiza archivos, procesos y memoria del sistema.
- Detecta, elimina o restaura
  Funciones habituales:
  - Detección por firmas
  - Análisis heurístico
  - Cuarentena
  - Eliminación o reparación de archivos infectados
- Si el ataque pasa el firewall → entra en juego el antivirus
  Si un archivo malicioso se descarga desde una web permitida, el firewall no lo bloqueará.
  Ahí es donde **el antivirus debe reaccionar**.

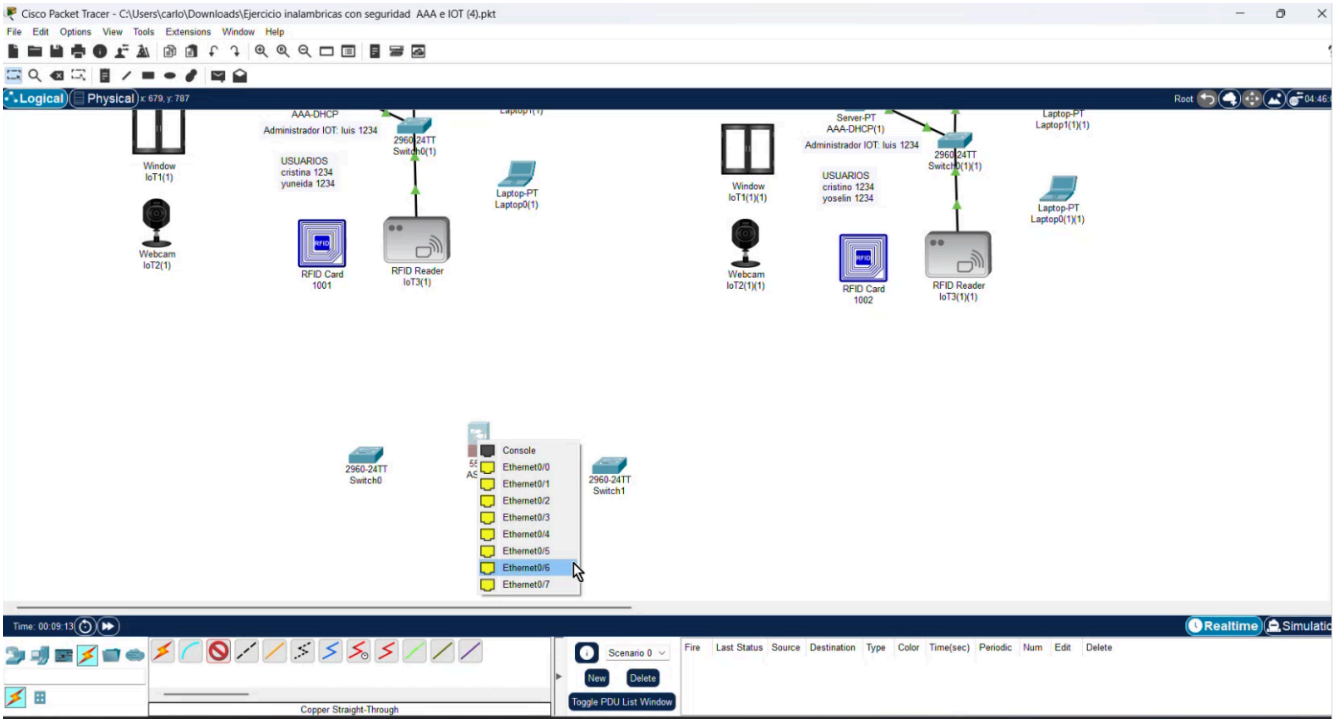
👉 Resumen rápido (muy de examen):
Firewall = portero del edificio
Antivirus = equipo de limpieza (cuando alguien se cuela)

3️⃣ Firewall físico Cisco ASA — Conceptos clave

El firewall **Cisco ASA** es un ejemplo típico de firewall **perimetral empresarial**, y se basa en el concepto de **zonas de seguridad**.

🔹 Interfaces físicas

- ASA dispone de **8 interfaces físicas**
- Numeradas de **Ethernet0/0 a Ethernet0/7**



Cada interfaz puede:

- Asignarse a una VLAN
- Tener un nivel de seguridad distinto
- Representar una zona de red diferente (inside, outside, DMZ, etc.)

📌 Importante:

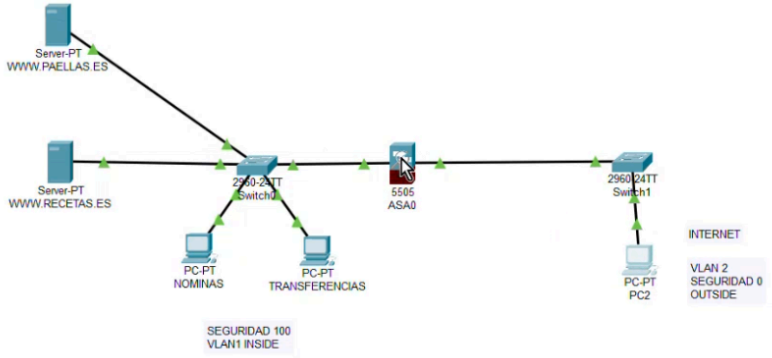
> En ASA, **las interfaces no son iguales**: su nivel de seguridad define cómo fluye el tráfico.

🔹 Niveles de seguridad

El ASA utiliza un sistema de **niveles de confianza** para controlar el tráfico.

- Rango de **0 a 100**
- **100 → zona más protegida**
- **0 → zona menos fiable (Internet)**

Zona	VLAN	Seguridad	Descripción
INSIDE	VLAN 1	100	Red interna, datos sensibles
OUTSIDE	VLAN 2	0	Internet / clientes



📜 **Ley básica del ASA:**

> Una red con **menor nivel de seguridad NO puede acceder** a una de nivel superior **por defecto**.

Esto implica:

- ❌ OUTSIDE → INSIDE bloqueado
- ✔ INSIDE → OUTSIDE permitido
- ❌ Ping desde fuera bloqueado sin reglas explícitas

👉 Esta política sigue el principio de **mínimo privilegio**.

4️⃣ Objetivo de la topología

El objetivo del ejercicio es **simular una situación empresarial real**.

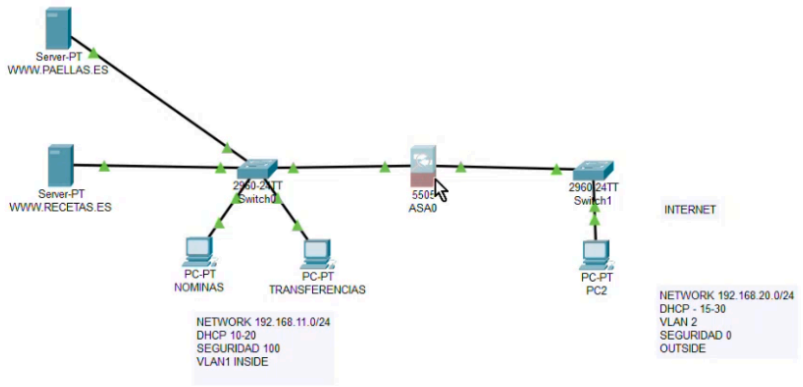
- Un cliente externo (**PC2 / Internet**) debe:
  - ✔ Acceder **únicamente a los servidores web**
  - ❌ NO acceder a **Nóminas** ni **Transferencias**, que contienen información crítica
- Todo el tráfico pasa obligatoriamente por el firewall:

```
Cliente → Firewall → Switch empresa → Servidores
```

📌 Punto clave:

> El cliente **nunca ve la red interna**, solo interactúa con lo que el firewall le permite.

5️⃣ Topología de red



🔹 Red INSIDE — Qué es y por qué se diseña así

- La red INSIDE representa **la red privada de la empresa**, es decir:
  - La parte **más confiable**
  - Donde están los **datos críticos**
  - La que **nunca debería estar expuesta directamente a Internet**
- En un entorno real, esta red equivaldría a:
  - Red de empleados

    - Red de servidores internos
    - Red financiera / RRHH
- En Cisco ASA, esta red se asocia a:
    - **VLAN 1**
    - **Nivel de seguridad 100**

👉 El valor **100 no es decorativo**:

- Indica al firewall que:
    - Esta red es de **máxima confianza**
    - El tráfico que sale desde aquí se permite por defecto
    - El tráfico que entra **se bloquea**, salvo reglas explícitas

---

🔹 Red INSIDE — Construcción física en Cisco Packet Tracer

1️⃣ Colocación de dispositivos

- Arrastras al escenario:
    - 1 switch (2960)
    - 2 PCs
    - 2 servidores
    - 1 firewall ASA 5505
- El orden visual **no es solo estético**:
    - Te ayuda a entender el flujo del tráfico
    - Facilita el debug posterior

2️⃣ Cableado interno (muy importante)

- Todos los PCs y servidores:
    - Se conectan **únicamente al switch**
- El switch:
    - Se conecta **a un solo puerto del ASA**

👉 A nivel de red esto significa:

- Los PCs **no pueden saltarse el firewall**
- No existe ningún camino alternativo
- Todo paquete:
    - Sale del PC
    - Llega al switch
    - **Debe pasar por el ASA**

📌 Si conectaras un PC directamente al ASA por error:

- Cambiaría su zona
- Cambiaría su nivel de seguridad
- Cambiaría su comportamiento

🔹 Red INSIDE — Direccionamiento IP explicado

- Red: `192.168.11.0/24`
  - Permite hasta 254 hosts
  - Más que suficiente para una LAN corporativa pequeña
- Gateway: `192.168.11.1`
  - Es la IP del **firewall**
  - No del switch
  - No de un router externo

👉 Esto implica:

- Todo tráfico que no sea local:
  - Va al ASA
- El ASA decide:
  - Si se enruta
  - Si se bloquea
  - Si se traduce (NAT en escenarios reales)

🔹 Servidores internos — Configuración y lógica

Por qué los servidores tienen IP fija

- Los servidores:
  - No deben cambiar de IP
  - Son puntos de acceso controlados
  - Se referencian en reglas del firewall
- En Packet Tracer:
  - Desktop → IP Configuration
  - Static
- Configuras:
  - IP (ej. 192.168.11.2)
  - Máscara
  - Gateway (ASA)

👉 Si el gateway fuera incorrecto:

- El servidor **recibiría peticiones**
- Pero **no sabría cómo responder**
- Desde fuera parecería “caído”

🔹 Red OUTSIDE — Qué representa realmente

- La red OUTSIDE **no es “Internet real”**, pero:
  - Lo simula
  - Se comporta como tal
  - Se trata con **desconfianza total**
- Se asocia a:

- VLAN 2
- Nivel de seguridad 0

👉 Nivel 0 significa:

- Ningún privilegio
- Ningún acceso por defecto
- Todo tráfico es sospechoso

🔹 Red OUTSIDE — Construcción en Packet Tracer

Dispositivos

- Un PC (PC2) representa:
  - Un cliente
  - Un usuario externo
  - Un posible atacante
- Un switch representa:
  - ISP
  - Red pública
  - Infraestructura fuera de tu control

Cableado OUTSIDE

- PC2 → Switch
- Switch → Puerto OUTSIDE del ASA

👉 Esto provoca que:

- Todo lo que salga del PC:
  - Entre al ASA por OUTSIDE
- El ASA:
  - Detecte que el tráfico viene de **zona 0**
  - Aplique reglas restrictivas

🔹 Qué ve el cliente externo (PC2)

- PC2 usa DHCP
- Recibe:
  - IP
  - Máscara
  - Gateway (ASA)

👉 Lo que **NO recibe**:

- Información sobre INSIDE
- IPs internas
- VLANs
- Servidores

📌 Desde su punto de vista:

- La empresa es **una sola IP**
- El firewall es “la empresa”

6️⃣ Configuración del Firewall ASA (CLI)

En este punto pasamos de la **teoría** a la **configuración real del firewall**, que será el **núcleo de control de toda la red**.
Todo el tráfico, tanto interno como externo, **dependerá de lo que configuremos aquí**.

🔹 Acceso inicial

```
ciscoasa> enable
ciscoasa# show run
ciscoasa# conf t
```

🧠 Explicación detallada

- `enable`
  🔐 Accede al **modo privilegiado** del ASA.
  Sin este modo **no se puede ver ni modificar la configuración**.
- `show run`
  📄 Muestra la **configuración activa en memoria**.
  Se utiliza para:
  - Ver cómo está configurado el firewall
  - Detectar configuraciones por defecto
  - Comprobar cambios tras cada paso
- `conf t` (configure terminal)
  ✍️ Entra en **modo configuración global**.
  A partir de aquí:
  - Se definen interfaces
  - Se configuran VLANs
  - Se habilita DHCP, WebVPN, usuarios, etc.

📌 **Idea clave**:

> Antes de tocar nada, **siempre se revisa el estado actual** del firewall.

🔹 Configuración DHCP INSIDE

Este bloque define **cómo el firewall asigna IPs automáticamente** a los equipos internos.

```
no dhcp address 192.168.1.5-192.168.1.36 inside
no dhcp enable inside
```

🧠 ¿Por qué se hace esto?

- El ASA viene con **DHCP por defecto**

- Usa rangos genéricos que **no coinciden con la red real**
- Si no se elimina:
  - Puede asignar IPs incorrectas
  - Provocar conflictos de red

📌 **Buenas prácticas empresariales**:

> Primero se elimina cualquier configuración automática que no controle la empresa.

```
interface Vlan1
 ip address 192.168.11.1 255.255.255.0
 exit
```

🌐 Qué ocurre a nivel de red

- Se configura la **VLAN 1 (INSIDE)**
- `192.168.11.1` pasa a ser:
  - ✔ Gateway de todos los PCs internos
  - ✔ Punto de salida hacia Internet
  - ✔ Punto de entrada a los servidores

📌 **Sin esta IP**:

- Los PCs no sabrían a dónde enviar tráfico externo
- No existiría enrutamiento

```
no dhcp address 192.168.11.10-192.168.11.20 inside
dhcp enable inside
```

🔄 Funcionamiento DHCP INSIDE

- Se define el rango:
  - Desde `.10` hasta `.20`
- El firewall:
  - Escucha peticiones DHCP
  - Asigna IP
  - Indica gateway (`192.168.11.1`)
  - Indica máscara

📌 **Ventaja clave**:

> El firewall **controla completamente la red interna**, no solo filtra tráfico.

📌 Tras refrescar DHCP:

- PCs reciben IPs **.10 y .11**

🧪 Esto confirma:

- DHCP funciona

- VLAN está operativa
- El ASA es el gateway real

🔹 Configuración OUTSIDE

Ahora se configura la **zona menos confiable**, que representa Internet.

```
no dhcp auto_config outside
```

⚠️ Importante

- `auto_config` crea una red automática
- En un entorno empresarial:
  - ❌ No se usan configuraciones automáticas
  - ✔ Todo se define explícitamente

```
interface Vlan2
 ip address 192.168.20.1 255.255.255.0
 exit
```

🌐 A nivel de red

- `Vlan2` pasa a ser la **zona OUTSIDE**
- `192.168.20.1` es:
  - Gateway del cliente externo (PC2)
  - Punto de entrada a la empresa

📌 **El cliente solo conoce esta IP**, nada más.

🔹 DHCP OUTSIDE

```
dhcp address 192.168.20.15-192.168.20.30 outside
dhcp enable outside
```

🔄 Qué sucede aquí

- El ASA actúa como:
  - Firewall
  - Router
  - Servidor DHCP externo
- PC2 recibe:
  - IP
  - Gateway
  - Acceso limitado según reglas

📌 **Detalle clave**:

> Aunque sea “Internet”, sigue estando **bajo control del firewall**.

7️⃣ Regla de seguridad fundamental del Firewall ASA

🔐 Principio básico de seguridad en Cisco ASA

> **Una interfaz con menor nivel de seguridad NO puede iniciar comunicación hacia una interfaz con mayor nivel de seguridad.**

En este laboratorio:

- **OUTSIDE**
  - Nivel de seguridad: **0**
  - Representa Internet / clientes
- **INSIDE**
  - Nivel de seguridad: **100**
  - Representa la red interna de la empresa

👉 Esta regla se aplica **automáticamente**, sin necesidad de crear ACLs.

🧠 Qué significa esto realmente (concepto clave)

El ASA **no es neutro**:
toma decisiones basadas en el **nivel de confianza de cada red**.

- Tráfico de **INSIDE → OUTSIDE**
  - ✅ Permitido por defecto
- Tráfico de **OUTSIDE → INSIDE**
  - ❌ Bloqueado por defecto

📌 Esto implementa el modelo:

> **“Confiar hacia fuera, desconfiar hacia dentro”**

🌐 Qué ocurre a nivel de red (sin reglas adicionales)

Cuando un paquete entra por la interfaz OUTSIDE:

1. El ASA identifica:
   - Interfaz de entrada
   - Nivel de seguridad (0)
2. Comprueba la interfaz de destino:
   - Nivel de seguridad 100
3. Compara ambos valores
4. Al ser **0 → 100**, el ASA:
   - ❌ Bloquea el paquete
   - ❌ No lo reenvía
   - ❌ No genera respuesta ICMP

📌 El bloqueo es **silencioso** (stealth).

❌ Ping bloqueado: explicación completa

🧪 Prueba en Cisco Packet Tracer

Desde **PC2 (OUTSIDE)**:

1. Desktop → Command Prompt
2. Ejecutar:

```
ping 192.168.11.10
```

🔍 Resultado

- El ping **no responde**
- Aparecen timeouts

🧠 Por qué ocurre

- El ping es tráfico **ICMP**
- ICMP también está sujeto a:
  - Niveles de seguridad
  - Reglas del firewall
- El ASA:
  - Recibe el paquete ICMP
  - Detecta origen OUTSIDE
  - Detecta destino INSIDE
  - ❌ Lo descarta

📌 Esto evita:

- Descubrimiento de hosts
- Mapeo de red
- Reconocimiento previo a ataques

❌ Acceso directo a PCs internos (bloqueo total)

🧪 Ejemplo realista

Desde PC2 intentar:

- Acceder por IP a:
  - PC Nóminas
  - PC Transferencias
- Intentar conexión TCP (HTTP, SMB, etc.)

🔒 Resultado

- ❌ Conexión imposible
- ❌ No hay respuesta
- ❌ El cliente no sabe si existe el equipo

🧠 Qué está protegiendo el ASA aquí

- Datos personales

- Datos financieros
- Sistemas críticos

👉 **Aunque conozcas la IP**, el firewall **no te deja ni llamar a la puerta**.

✔ Tráfico permitido explícitamente (la excepción)

El único tráfico que puede pasar de OUTSIDE a INSIDE es aquel que:

- ✔ Está **definido explícitamente**
- ✔ Está **publicado por el firewall**
- ✔ Está **asociado a una política**

Ejemplo en este laboratorio:

- WebVPN
- Bookmarks
- Acceso autenticado

📌 Nada entra “porque sí”.

🔑 Concepto clave: *Deny by default*

Este comportamiento se resume en:

> **Todo está prohibido salvo lo que se permita expresamente**

Esto implica:

- Menor superficie de ataque
- Menos errores humanos
- Mayor control

📌 Este principio es la base de:

- Firewalls empresariales
- Zero Trust
- SOC
- Arquitecturas modernas de seguridad

🧪 Qué pasaría si cambiamos los niveles (teórico)

Si OUTSIDE tuviera nivel 100 y INSIDE 0:

- OUTSIDE podría:
  - Hacer ping
  - Acceder a PCs
  - Acceder a servidores

👉 Sería un **diseño inseguro** y **antiprofesional**.

Por eso:

- Internet siempre es 0

- La red interna siempre es alta

🧱 Relación directa con el mundo real

En empresas reales:

- OUTSIDE = Internet
- INSIDE = red corporativa
- DMZ = nivel intermedio (no visto aún)

📌 El ASA actúa como:

- Guardia
- Filtro
- Punto de decisión

8️⃣ Publicación de servicios mediante WebVPN (AAA)

En este punto el laboratorio da un salto clave:
pasamos de **"bloquear todo"** a **"permitir solo lo necesario"**, aplicando **AAA (Authentication, Authorization, Accounting)**.

🔐 ¿Por qué se usa WebVPN y no abrir la red?

Antes de configurar nada, hay que entender **la idea de fondo**:

- **NO** se quiere:
  - Dar acceso a la red interna
  - Permitir tráfico libre desde Internet
  - Exponer IPs internas
- **SÍ** se quiere:
  - Permitir acceso a **servicios concretos**
  - Identificar **quién accede**
  - Controlar **a qué accede cada usuario**

👉 WebVPN permite exactamente eso:
acceso por aplicación + por usuario, no por red.

🧠 Qué es WebVPN en Cisco ASA (conceptualmente)

WebVPN en ASA es:

- Un **portal web seguro (HTTPS)**
- Gestionado directamente por el firewall
- Que:
  - Autentica usuarios
  - Aplica políticas
  - Redirige tráfico interno de forma controlada

📌 Importante:

> **No es una VPN completa** (no crea túnel de red).
> Es **una VPN de acceso web**.

🖱️ Configuración gráfica en Cisco Packet Tracer (paso a paso)

📍 Dónde se configura

1. Click en **Firewall ASA**
2. Pestaña **Config**
3. Menú lateral → **WebVPN**

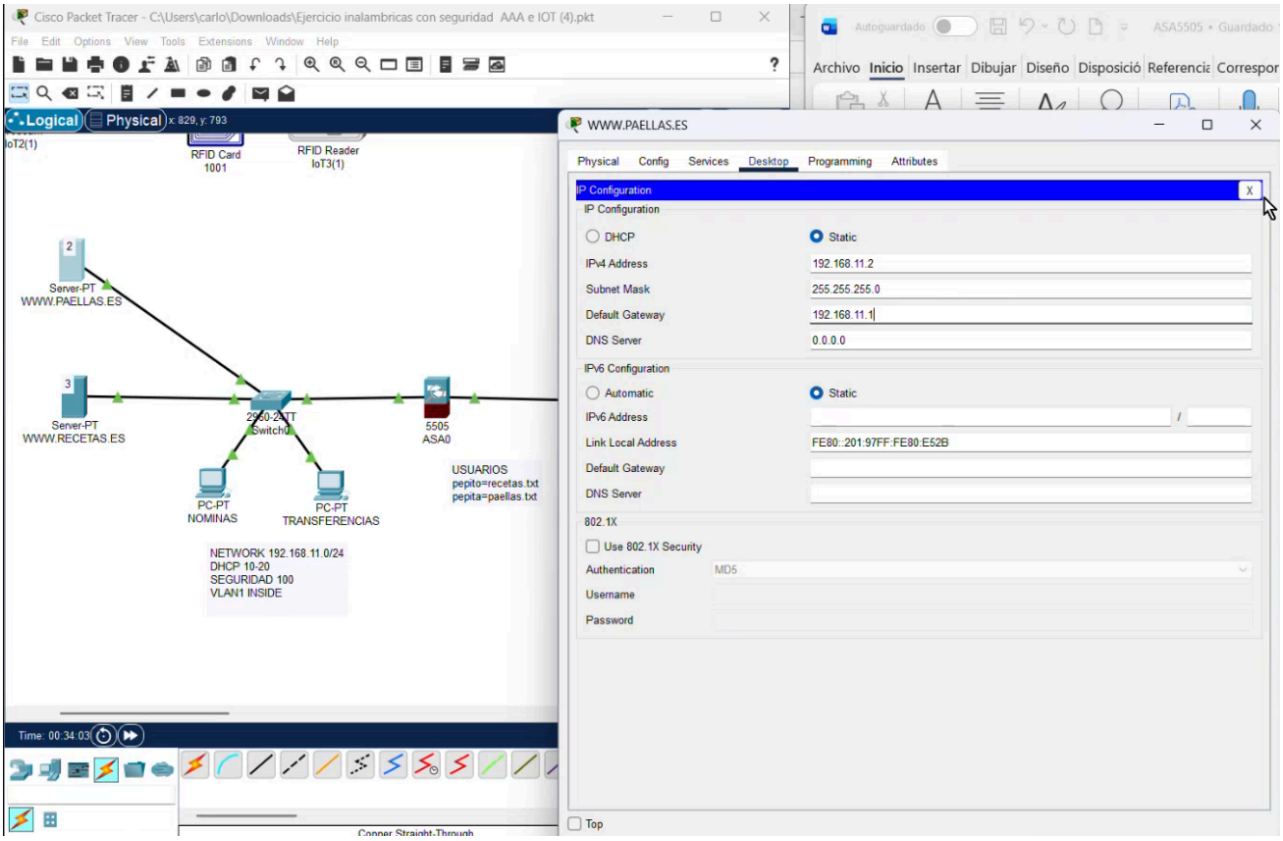
Aquí **NO usas la CLI**, sino la interfaz gráfica del ASA en Packet Tracer.

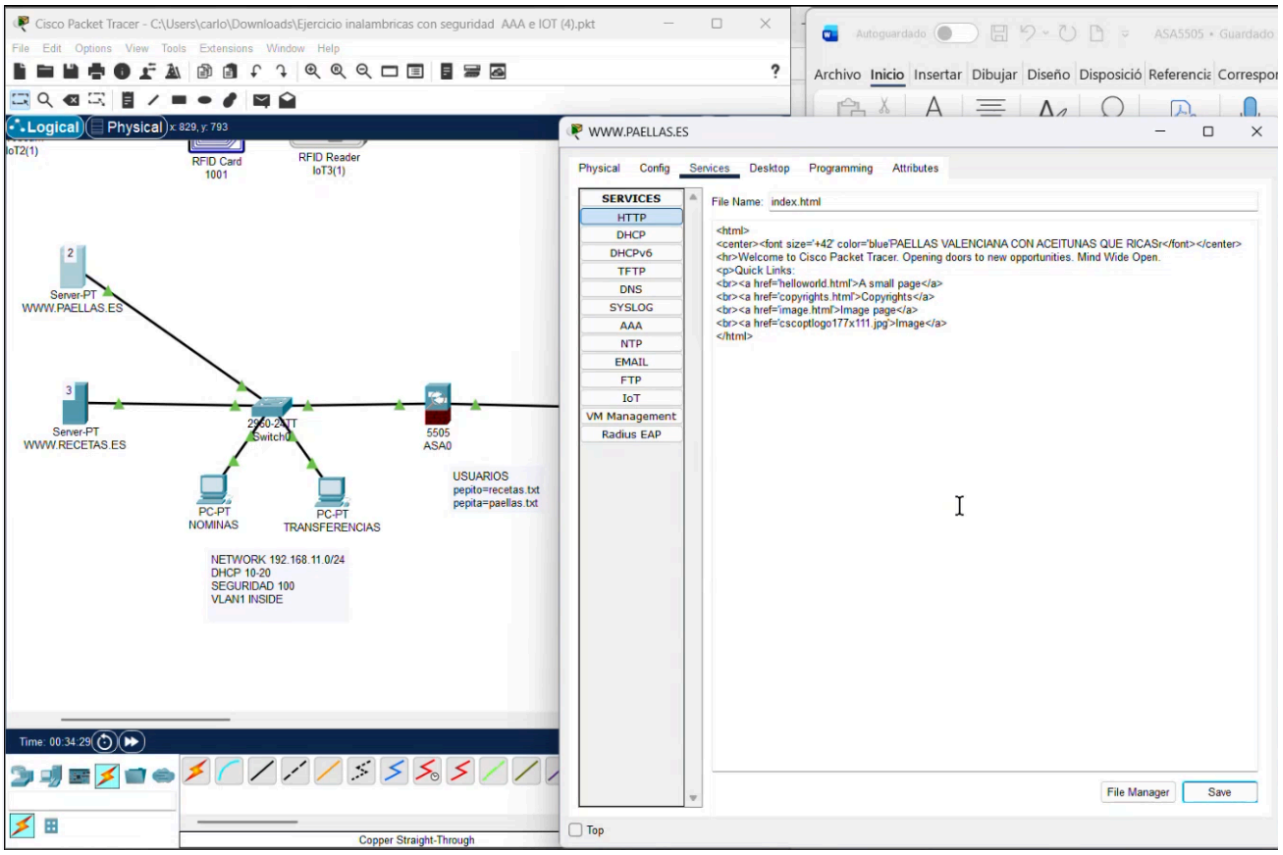
🔹 Bookmarks — Qué son y por qué son clave

Los **Bookmarks** son:

- Enlaces web internos
- Publicados por el firewall
- Asociados a usuarios o grupos

👉 El usuario **no navega libremente**:
solo puede acceder a los enlaces que tú definas.





🔹 Bookmarks configurados

Servicio	IP interna	Función
www.paellas.es	192.168.11.2	Web interna
www.recetas.es	192.168.11.3	Web interna

🧠 Qué ocurre a nivel de red con un Bookmark

Cuando un cliente accede a un bookmark:

1. El navegador se conecta al **ASA** (HTTPS)
2. El ASA:
   - Recibe la petición
   - Comprueba el usuario
3. El ASA:
   - Hace de **proxy**
   - Contacta con el servidor interno
4. El servidor responde al ASA
5. El ASA devuelve la respuesta al cliente

📌 El cliente:

- ❌ Nunca conecta directamente al servidor
- ❌ Nunca ve la IP interna
- ✔ Solo habla con el firewall

🔹 Activación de WebVPN (CLI)

```
conf t
webvpn
 enable
 enable outside
```

🧠 Explicación comando a comando

- `webvpn`
  Entra en el modo de configuración del portal WebVPN.
- `enable`
  Activa el servicio WebVPN.
- `enable outside`
  Indica que:
  - El portal será accesible
  - Desde la interfaz **OUTSIDE**
  - Es decir, desde Internet

📌 Sin `enable outside`:

> El portal existiría, pero **nadie podría acceder desde fuera**.

🔹 Creación de usuarios (AAA — Authentication)

```
username pepito password 1234
username pepita password 1234
```

🔐 Qué significa esto realmente

El firewall pasa a:

- Tener **usuarios locales**
- Poder:
  - Autenticar personas
  - Diferenciar accesos
  - Aplicar políticas personalizadas

👉 El ASA deja de ser solo:

- Router
- Firewall
  y pasa a ser **sistema de control de identidad**.

🔹 Asignación de perfiles y grupos (Authorization)

Usuario	Web permitida	Perfil	Grupo
pepito	paellas.es	Vpepito	Gpepito
pepita	recetas.es	Vpepita	Gpepita

🧠 Qué son perfiles y grupos

- **Perfil (Profile)**:
  - Define qué puede hacer el usuario
  - A qué recursos accede
- **Grupo (Group Policy)**:
  - Conjunto de reglas
  - Permite escalar a muchos usuarios

📌 En empresas reales:

- No se gestiona usuario por usuario
- Se gestionan **grupos y roles**

🧠 Qué ocurre cuando un usuario inicia sesión

1. El usuario introduce credenciales
2. El ASA:
   - Verifica usuario y contraseña (Authentication)
3. El ASA:
   - Asigna perfil y grupo (Authorization)
4. El ASA:
   - Muestra solo los bookmarks permitidos

👉 Resultado:

- **Pepito NO ve recetas**
- **Pepita NO ve paellas**

🔒 Accounting (el tercer A, aunque no se vea)

Aunque Packet Tracer no lo muestra en detalle, conceptualmente:

- El ASA podría registrar:
  - Quién accede
  - Cuándo
  - A qué servicio
  - Durante cuánto tiempo

📌 Esto es fundamental en:

- Auditorías
- SOC
- Incidentes de seguridad

🧪 Prueba práctica desde el cliente (PC2)

Paso a paso

1. Abrir navegador web en PC2
2. Acceder a:

```
https://192.168.20.1
```

3. Aparece el portal WebVPN
4. Introducir usuario:
   - pepito / 1234
   - o pepita / 1234

Resultado según usuario

- **Pepito**:
  - Solo ve `www.paellas.es`
  - Accede correctamente
- **Pepita**:
  - Solo ve `www.recetas.es`
  - No puede acceder a paellas

📌 Esto demuestra:

> **Control por identidad, no por IP**

🔐 Seguridad que aporta WebVPN

Gracias a esta configuración:

- ❌ No se abre INSIDE
- ❌ No hay acceso a PCs internos
- ❌ No hay exploración de red
- ✔ Acceso mínimo y controlado

👉 Principio aplicado:

> **Least Privilege** (mínimo privilegio)

🎯 Conclusión del punto 8

- WebVPN permite:
  - Publicar servicios internos
  - Sin exponer la red
  - Con control total por usuario
- El firewall:
  - Filtra tráfico
  - Autentica usuarios
  - Autoriza accesos
  - Centraliza la seguridad

👉 Este modelo es:

- Empresarial
- Realista

- Base directa de:
  - Zero Trust
  - SOC
  - Arquitecturas modernas

9️⃣ Funcionamiento final del sistema (visión cliente y visión firewall)

En este punto ya **no se configura nada más**.
Aquí se analiza **qué ocurre realmente cuando el sistema está en producción**, exactamente como lo ha diseñado el profesor.

🔍 9.1 Visión del cliente externo (PC2)

🖥️ Qué sabe el cliente

Desde el punto de vista del **PC2**, el usuario externo:

- ✔ Conoce **una única IP**:
  - `192.168.20.1` → el firewall
- ❌ No conoce:
  - La red INSIDE
  - Las IPs `192.168.11.x`
  - Cuántos servidores existen
  - Qué PCs internos hay

👉 Para el cliente:

> **La empresa es el firewall**.

🌐 Qué puede hacer el cliente

El cliente solo puede:

- Abrir un navegador web
- Conectarse por HTTPS al ASA
- Introducir credenciales

Todo lo demás:

- ❌ Ping
- ❌ Escaneo
- ❌ Acceso directo
  está bloqueado.

🔐 9.2 Flujo completo de conexión (paso a paso real)

Vamos a describir **exactamente** qué pasa cuando el cliente accede a un servicio.

1️⃣ El cliente inicia la conexión

- El usuario abre el navegador
- Introduce:

```
https://192.168.20.1
```

📡 A nivel de red:

- Se genera un paquete HTTPS
- Destino: IP del ASA
- Entra por la interfaz **OUTSIDE**

2️⃣ El ASA recibe el tráfico

El firewall:

- Detecta:
  - Interfaz de entrada: OUTSIDE
  - Nivel de seguridad: 0
- Permite el tráfico porque:
  - WebVPN está habilitado
  - HTTPS está permitido hacia el propio ASA

📌 Importante:

> El cliente **no entra en INSIDE**, solo habla con el firewall.

3️⃣ Autenticación (Authentication)

El ASA:

- Muestra el portal WebVPN
- Solicita:
  - Usuario
  - Contraseña

Cuando el usuario envía las credenciales:

- El ASA:
  - Comprueba si el usuario existe
  - Verifica la contraseña

❌ Si falla:

- Acceso denegado
- No se muestra ningún recurso

✔ Si acierta:

- Se pasa al siguiente paso

4️⃣ Autorización (Authorization)

Una vez autenticado, el ASA:

- Asocia el usuario a:
  - Un perfil
  - Un grupo
- Consulta:
  - Qué bookmarks tiene permitidos

📌 Aquí ocurre algo clave:

> **Dos usuarios, mismo firewall, resultados distintos**

5️⃣ Presentación de recursos (Bookmarks)

Según el usuario:

- **pepito**
  - Ve solo: `www.paellas.es`
- **pepita**
  - Ve solo: `www.recetas.es`

El cliente:

- ❌ No puede escribir otra URL
- ❌ No puede cambiar el destino
- ❌ No puede navegar libremente

Todo está **predefinido**.

6️⃣ Acceso al servidor interno (proxy del ASA)

Cuando el usuario hace clic en un bookmark:

- El navegador:
  - Sigue hablando **solo con el ASA**
- El ASA:
  - Actúa como **proxy**
  - Inicia una conexión interna hacia:
    - `192.168.11.2` o `192.168.11.3`

📡 A nivel de red:

- OUTSIDE → ASA (HTTPS)
- ASA → INSIDE (HTTP/HTTPS interno)

📌 El cliente **nunca se conecta directamente** al servidor.

7️⃣ Respuesta del servidor

El servidor interno:

- Recibe la petición del ASA
- Responde normalmente

- Usa como gateway:
  - `192.168.11.1` (el ASA)

El tráfico de vuelta:

- Pasa por el ASA
- Se encapsula en la sesión WebVPN
- Se envía al cliente

🧱 9.3 Qué NO ocurre (muy importante)

Gracias a esta arquitectura:

- ❌ El cliente no puede:
  - Hacer ping a INSIDE
  - Escanear puertos internos
  - Ver PCs de nóminas o transferencias
  - Saltarse el firewall
  - Cambiar de servidor

📌 Esto no depende del usuario:

> Depende **del diseño de red y del firewall**.

🔒 9.4 Seguridad aplicada en este punto

En este funcionamiento final se aplican varios principios clave de seguridad:

- 🔐 **Perimeter Security**
  Todo pasa por el firewall
- 👤 **Security by Identity**
  El acceso depende del usuario, no de la IP
- 🚫 **Deny by Default**
  Nada entra si no está permitido
- 🎯 **Least Privilege**
  Cada usuario ve solo lo que necesita

🧠 9.5 Relación directa con entornos reales

Este modelo es **exactamente** el que se usa en:

- Acceso remoto a aplicaciones corporativas
- Portales internos publicados
- Entornos SOC
- Arquitecturas Zero Trust

📌 En el mundo real:

- El ASA podría enviar logs a un SIEM
- Registrar accesos
- Detectar anomalías

🔚 Conclusión

- El **firewall físico** es el pilar de la seguridad perimetral
- Los **niveles de seguridad** definen qué tráfico está permitido
- **AAA + WebVPN** permite:
  - Controlar acceso
  - Segmentar usuarios
  - Publicar servicios sin exponer la red interna
- Este modelo es **realista y empresarial**, y encaja directamente con:
  - 🔐 SIEM HomeLab
  - 🧠 SOC / Blue Team
  - 🏢 Redes corporativas reales

📌 *El firewall lógico se verá más adelante con VirtualBox.*